CSCI301 Assignment 2 Report

Done by: Colemann Gee Wei Shaun

7311369

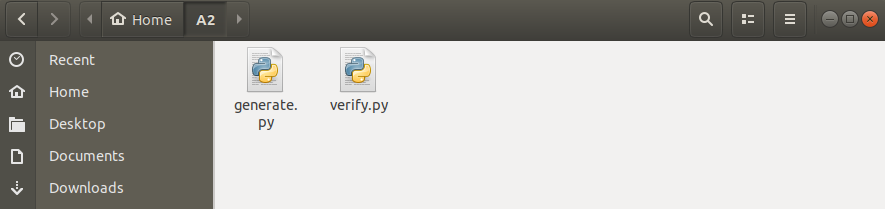
Python version used

* 3.6.9

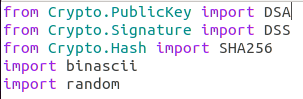
Requirements to run the code:

* Python 3.5 or above
* Pycryptodome pakages installed

An example directory for seamless execution:

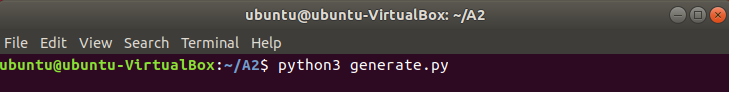


All imports used:

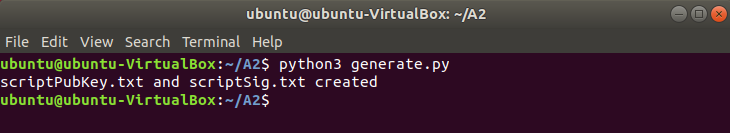


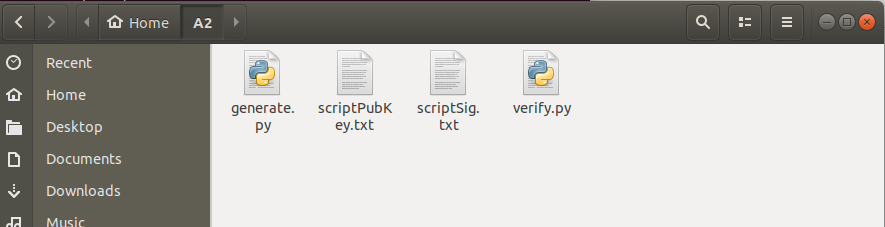
The python file generate.py is the program used to generate the scriptPubKey.txt and scriptSig.txt files.

generate.py is executed but running the following command

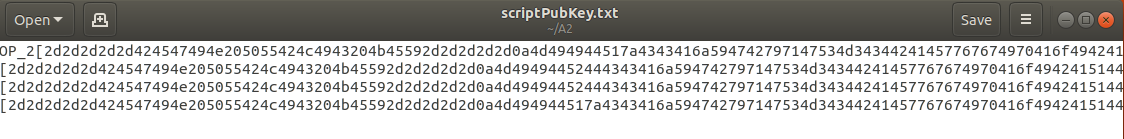


Upon seeing the following feedback, the 2 text files will be created

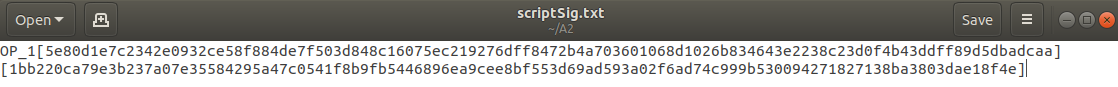




Example contents of scriptPubKey.txt file (Truncated as it does not fit the window):



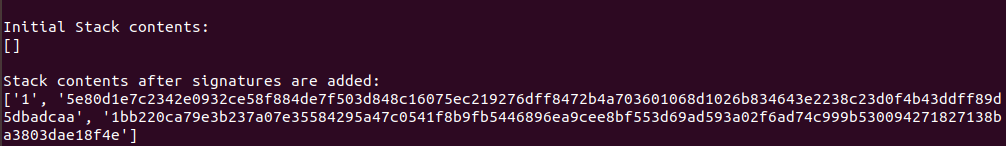
Example contents of scriptSig.txt file:



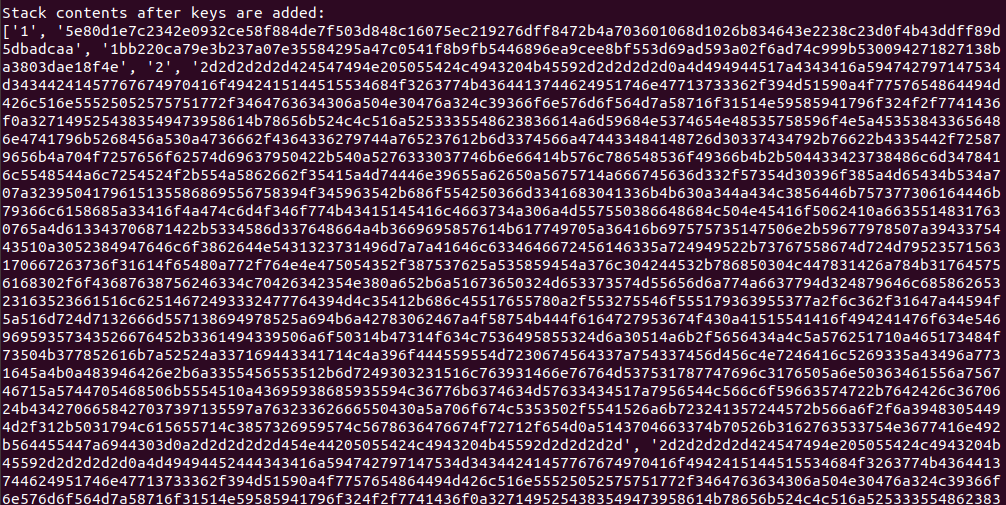
Next, the verify.py file can be executed by running the following command:

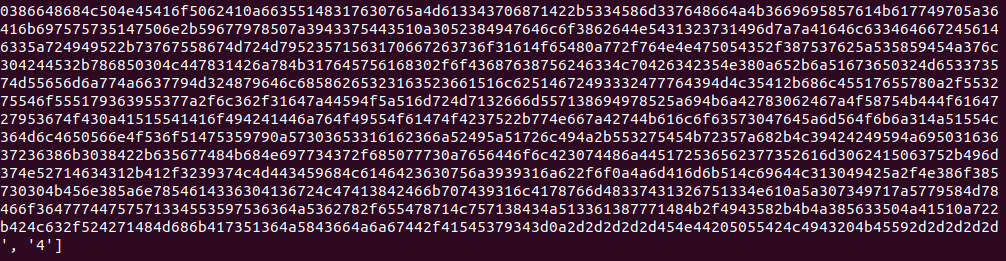


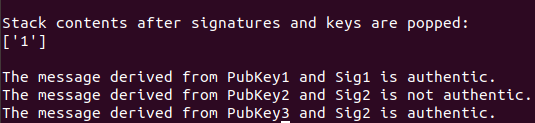
Example of the results that will be printed out:



Contents in “Stack contents after keys are added:” are truncated in the screenshots as seen in the following 2 screenshots.







The verification results in this example show that pubkey 1 and pubkey 3 were used in the signing of the message.